



Renaud, K. and Cockshott, W.P. (2007) *Electronic plebiscites*. In: MeTTeG07, 27-28 September 2007, Camerino.

<http://eprints.gla.ac.uk/4483/>

Deposited on: 7 April 2009

ELECTRONIC PLEBISCITES

Karen Renaud, Paul Cockshott

University of Glasgow Dept Computing Science 17 Lilybank Gardens Glasgow

karen@dcs.gla.ac.uk wpc@dcs.gla.ac.uk

Abstract – We suggest a technology and set of procedures by which a major democratic deficit of modern society can be addressed. The mechanism, whilst it makes limited use of cryptographic techniques in the background, is based around objects and procedures with which voters are currently familiar. We believe that systems like this hold considerable potential for the extension of democratic participation and control.

1. – Introduction

Current political systems tend to have a very limited degree of democracy. Such control as the people have over public policy is indirect — mainly taking the form of periodic elections of popular representatives to the parliament. This form of indirect representation contrasts with the direct democracy that operated in ancient Greece where the entire citizen body would gather in the town square to debate and vote on issues which affected them [1, 2]. The ancient states of Greece were little more than we would now call towns, and techniques that worked for a town became impossible in a modern nation state. A nation cannot physically gather its population into one place to deliberate on policy.

At the time it was introduced, the right to vote for representatives in parliament was a big step forward. It was clearly better than having a parliament in which MPs were essentially appointed by the local aristocracy, but, when compared with direct democracy it has inherent weaknesses.

During the lifetime of a parliament, an MP, let us call here Ms Gray, will vote on perhaps 100 different items of legislation. Even if we suppose that the system that elected Ms Gray was fair, all this means is that a majority of her constituents preferred Ms Gray to her rivals Mr Red, Ms Green, and Mr Black. It does not follow that each time Ms Gray votes in the Parliament, her vote will represent the wishes of a majority of her constituents. That would only occur if the population at large lined up neatly into political parties, with all Labour voters agreeing with every act brought forward by a Labour government, and all Tory voters agreeing with every act of their own government. It is quite possible that the parliament will enact laws with which a majority of the population disagree.

On information theoretical grounds this is clearly deficient. Suppose elections are held every 4 years and that there are 8 candidates per seat. Each vote cast conveys $\text{Log}_2(8)=3$ bits, giving a bandwidth from each constituency to the political decision making process of only $\frac{3}{4}$ bit per year. But if an MP will make 25 yes/no votes per annum, there is thus clearly a huge “impedance mismatch” in the channel.

On very major constitutional issues, national referenda or plebiscites are held. Their infrequency stems both from their complexity and expense, and also from the reluctance of elected politicians to give up any of their power to the people they are supposed to represent.

Contrast this to what happens on TV. Every week there are reality TV shows, or competitions in which the viewers are asked phone in to decide which contestant is to win or loose. What makes them worth doing, from the TV companies' point of view, is that they are able to charge viewers phone bill every time they vote. What has made them possible is the digital technology which allows incoming phone calls and Short Text Messages to be rapidly counted. Commercial interests have resulted in a technology being developed, which, if applied in the field of national politics, would give citizens real democratic control over the executive.

Before the phone voting used on TV could be used in anything other than games, something would have to be done to make it not just efficient, which it already is, but secure, which it certainly is not. In TV phone voting, there is nothing to stop you voting as often as you wish for the candidate of your choice, provided that you are willing to pay the charge.

If this were the only problem with phone voting, there would be an easy answer, simply design the vote counting software so that it only counts a single vote from each phone, but this would not prevent somebody with both a land-line and a mobile phone from voting twice. If everyone trusted the state one solution would be for voters to register their phone number when they registered to vote. This would ensure one person one vote, but what if you feared the government? Would you not be afraid that they could now easily find out how you had voted? Might that information affect the way the government dealt with you in the future?

What is needed is a way of identifying each voter so that (s)he can only vote once, but at the same time preventing the government from discovering how (s)he voted.

2. – E-Voting Requirements

Any vote must guarantee both voter anonymity and integrity of the process [3]. A paper based process satisfies these requirements but is expensive and somewhat error prone since it relies on humans counting votes. There has been a move to electronic voting in some countries. Evans and Paul cite a report by the Caltech/MIT Voting project [4] which claims that only 1% of the US population used a paper ballot in 2000.

Unfortunately, whereas people have long experience with paper ballot, and therefore trust them, electronic voting has had some bad press and therefore voters tend to be rather cynical about it. One wants to avoid, at all costs, the secrecy that has bedevilled electronic voting in the USA where it led to suspicion that the voting machine firms, who sympathise with the Republican party, could have rigged the results of elections. The trio goals of anonymity, auditability and integrity encompass a number of requirements of e-voting systems. *Anonymity* [5] — voters should not be linked to their vote in case this could be used against them at a later stage. Assurances from those in power may well not be sufficient to reassure voters; the system must be demonstrably and verifiably anonymous; *Privacy & Confidentiality* [6, 7, 8] — voters should be able to record their vote without other voters or officials being able to observe them; *Coercion resistance* — the process should be resistant to coercion [5, 8]; *Verifiability* [5, 9, 7, 10] — this should be engendered by a transparent and open process which encourages voters to trust the system; *Lowering of barriers* [11] — there should be multiple ways for the voter to cast his or her vote, by means of various devices, so that both house-bound voters and travelling voters are accommodated, for example.

We also have to satisfy traditional transactional requirements [6] including *atomicity* [12] — one person, one vote; *integrity* [11, 7] — the person's vote must be recorded correctly and the

votes must be counted correctly; *durability* — votes should not be discarded; and *non-interference* [12] — it should not be possible for votes to be altered en-route to the vote storage system.

3. – The Proposed Voting Mechanism



Figure 1: Voter Card

As mentioned in the previous section, voting involves three distinct stages: registration, voting and verification. These are the stages the voter is involved in, but in order for the process to meet our two requirements, we need also to regulate the preparatory process and the required infrastructure. We will discuss our proposal in terms of how it will be implemented in these stages.

3.1 – Preparation

Voter cards will be produced for every voter in the country. This looks like a credit card with an embedded chip in it and a voter number printed on it. The voter number on each card is unique, and imprinted on the chip. There is also a PIN printed on the card, which may be needed for some input devices. Furthermore, on the back of the card, three telephone numbers are printed: A “Yes” number and a “No” number. (These are to facilitate SMS voting. These numbers will also be advertised by radio, television and newspaper in the run up to the plebiscite) A free help number is printed on the back of the card so that voters can have their votes voided if they voted in error or if they were coerced

3.2 – Registration

We would suggest that there be a fixed period during which people have to register to vote. This might for example be at 3 year intervals. We envisage that there would be multiple plebiscites between registration periods. Registration would happen as follows:

1. When you register, you present your identification, which is copied and then returned to you. Your name is ticked on the list of electors.
2. You then pick one of a number of sealed envelopes from a jar and thus receive one voter’s card in the sealed envelope. Most importantly for anonymity, the electoral officials cannot match the card number to the voter.

3. At the registration office a machine will be made available for voters to specify their voting preferences. For example, if the voter is concerned about being coerced, she/he could insert the card into the machine and tailor it so that the vote can only be cast from a polling booth.

4. Finally, at the end of the registration period election officials must enter the numbers of all remaining cards into the system so that no one can “steal” the votes associated with these cards.

5. On the registration closing date, a list of all the valid numbers will be recorded at an independent website called the “Validation Centre”, with an associated web service. This will be used for verification purposes once the votes are counted.

3.3 – Voting

Since one of the requirements of effective e-voting is the lowering of barriers, there should be a number of ways the voter can choose to register his/her vote:

- At the polls — the voter enters the booth, inserts his or her card into the slot and chooses yes or no. In order to accommodate illiterate users votes should be entered by means of a touch sensitive screen where options are clearly shown both textually and by means of icons.
- Via their ATM machine — the voter inserts the card into their bank’s ATM machine and registers their vote by choosing the option on the screen. The bank uses a secure channel to send the vote to the central voting system.
- Via public telephone kiosks — the voter enters the card into the slot below the phone. This causes an automatic and free call to be placed to the voting system and the user can then register the YES or NO vote either verbally or by choosing an option from the keypad as prompted. We suggest that the call is automatically placed to eliminate errors in entering the free phone numbers, which will be hidden since the card has been inserted into the kiosk. It is far simpler for a person register a Yes or No choice than to enter a 10 digit number.
- Via SMS — the voter sends an SMS message to the applicable number (Yes or No) with simply the voter card number embedded in the message. The system will request the PIN by SMS and the voter replies with an SMS with the PIN in it.
- Via a phone, either mobile or fixed line — the voter dials the advertised number and reads or keys in their voter number as prompted by the system. The system then requests the PIN and the user reads the PIN into the receiver.

The latter two (phone) options are the only ones where the voter identity can be discovered if the system records the caller identity. The voter card will carry instructions to the voter to hide their caller identity if this option is used. Furthermore, in order to prevent people sending votes in by simply guessing other people’s voter numbers, the voters using phone ballots will be required to give the matching PIN when they submit their vote via SMS or land line. This proves that they actually possess the card.

Note that the use of a PIN plus a voter number is in security terms equivalent to having just a longer number. Splitting it into two portions has advantages from the point of view of usability and reliability though because errors can be made keying in a number, and the probability of making a mistake is higher with one long number than two short numbers as we are better equipped to visually identify errors in short numbers than long numbers. Furthermore, people are familiar with PIN numbers and credit card security codes which carry out the same basic function.

3.4 – Verification

In order to prevent fraud in the counting process, the electoral commission will publish, on its website and on a specially designated TV channel, all the yes voter numbers and all the no voter numbers. If a voter wishes to check that her vote was correctly registered, and she has a computer with Internet access, she downloads the file onto her computer and uses an editor program to search for her number in either the YES file or the NO file. Alternatively, she tunes her TV to the designated channel and waits until her number comes up and checks that the vote recorded against that number is correct.

Publication of this list of votes allows independent verification of the count of votes cast for each proposition. This avoids the secrecy that has bedevilled electronic voting in the USA where it leads to suspicion that the voting machine firms, who sympathise with the Republican party, could have rigged the results of elections.

3.5 – Infrastructure

There is one major system involved in recording the votes and performing the counting process once the plebiscite is over. The system needs to be secured very carefully and all accesses to the system need to be made via a Virtual Private Network (VPN) connection. Therefore we will have a specialised system that interfaces with each of the input devices. The connection to each of these will occur via recognised channels and based on the requirements of the input device. These systems will communicate, via VPN, with the voter registration system. There will also be two specialised output handling systems to send the lists of voter numbers and choices to a website and TV channel. The communication with these systems will also be via VPN. All support and IT staff have to be very carefully vetted to ensure that they are above reproach.

3.6 – Audit

Once all voting has been completed, an audit process will verify that the votes have indeed been counted correctly. It should be possible to identify any insider interference at this stage and to narrow down the culprit in the case of fraudulent activity being uncovered.

4 Threats

It should be noted that in a system of plebiscites there is less at stake in each vote than there is in elections. In elections one has to face the risk of organised fraud perpetrated by political parties or politicians who have a lot to win or lose. In an individual plebiscite special interest groups may attempt to influence the vote, but such groups formed to fight one issue are less likely to have the nation-wide network of organised supporters that a political party has. The exception might be if a plebiscite was called that threatened the interests of some large business group — tobacco companies for example in the case of a proposal to ban smoking. Such organisations might make up in wealth what they lacked in terms of mass membership and still pose a danger to the procedures. But since such circumstances will be exceptional, the level of security need not be as high as for electronic elections.

Suppose we have a voting population of 100million. Except in very tightly fought issues, one would probably have to cast several million false votes to have a chance of changing the outcome of a vote. One has to provide sufficient safeguards to ensure that it is unlikely that fraud on this scale could go undetected.

Here are some threats to the process that need to be considered:

Preparation

Insider: Someone working at the manufacturing site may well record the numbers on some of the cards. If the card is issued to a voter and the insider has abused his knowledge to “steal” the person’s vote, the legitimate card holder will detect this as soon as he tries to vote and he will be able to contact the help number to void the vote already cast. If this occurs there are two options — either void the card number altogether and issue the voter with a new card, or simply void the vote and allow the voter to place his vote. The former is probably more secure but infeasible.

Outsider: Someone could bombard the system with 10 digit numbers in the hopes of being able to guess a valid voter card number. This is an inherent weakness of the phone-in input devices which we include to lower barriers to voting. The use of a separate PIN alleviates this threat to a certain extent since we could “lock” the card if the voter makes a number of errors with the PIN entry and require the legitimate voter to report to a polling station to correct the error.

Registration

Insider: One of the election officers could theoretically steal a card, but this is prevented by requiring a copy of the voter’s identification document to be made for each card issued.

Outsider: Someone could attempt to register by using a fake identity document. This threat is common to all voting mechanisms and cannot be alleviated by our proposal.

Voting (Outsider)

It is possible for someone to coerce the voter and to vote on his behalf. We have built two safeguards into the system to alleviate this:

- The voter can contact the authorities and have the vote voided
- The voter can, at registration, request that the vote only be accepted from a polling booth where she can be protected from coercive activities.
- A voter card may be stolen and used by the thief to place a vote they are not entitled to. Since the card is not linked to the voter there is no way for the system to void such votes unless the user has recorded both the voter card number and the PIN and is able to give the electoral officer this information. Even if a voter proffers such information one has no way of knowing whether this is a valid complaint or an attempt to void someone else's vote.
- Brute force: someone could write code to flood the system with guessed voter card numbers to register false votes. This will not work unless they can guess the matching PIN and the chances of this happening are 1 in 10000 for a 4 digit PIN.

Verification (Outsider) — Someone could hack into the website and insert fictitious numbers into the files. This could be alleviated by having updating this list at regular intervals from the vote recording site.

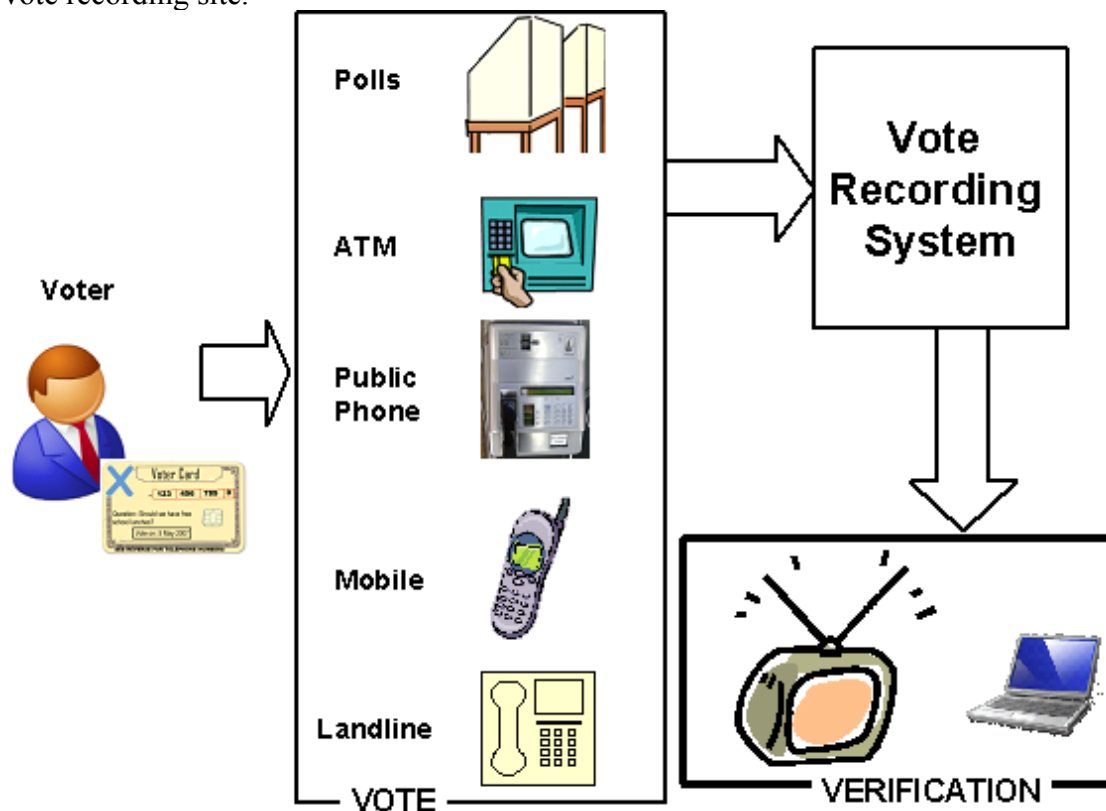


Figure 1: Voting Infrastructure

Environment (Insider)

- Someone could insert a vote into the system using a legitimate voter number. This is alleviated by means of the continuously updated verification lists and the ability to void votes, upon request.
- Somebody could fraudulently add voter card numbers and PINs to the list which corresponded either to cards which were never handed out, or to cards which never existed. With the use of these numbers they could then make fraudulent votes.

In order to guard against fraudulent insiders of the latter type we propose the following procedures:

- When voting cards are manufactured, 4 plain text copies of the list of valid cards are made: one on paper and three on some archival machine readable medium. The paper copy and one machine readable copy are sealed and placed in a secure bank vault under the view of witnesses. It is important that only a small number of known individuals participate in this process.
- The machine readable copies are then transferred to a Validation Centre where an encrypted copy is made and placed on a secure server. One copy is a backup in case of media errors. Having been encrypted the plain text archival media are then publicly destroyed. It is important that only a small number of known individuals participate in this process.
- Electoral registration officers return plain-text copies of the list of unused voter cards to the validation office and also publish these lists of unused voter cards.
- The vote counting computers are run by an organisation distinct from the Validation Centre. When votes occur, voter numbers that have been phoned in are checked, over a secure channel, with the Validation Centre, after having first been checked against the published list of unused voter cards. The Validation Centre returns a yes/no for each query.

Audit

At the end of the 3 year registration period, the sealed copies of the original list of cards are opened and the list of cards that were originally valid is published. Since all votes cast have also been published, it is possible for any private organisation with modest computing facilities to check if any of the published votes cast in the last 3 years were by cards that had not been validly issued. In the case of a discrepancy the suspicion would fall on a small group of known individuals. The near certainty of malfeasance detection should be an incentive adequate to ensure honesty in this group.

5 Comparison with other proposals

Most other proposals for electronic voting are concerned with elections rather than plebiscites. As we have argued, the former require higher levels of security. Another important factor is that in a system of participatory democracy voting will be more frequent and must therefore be more accessible. Our proposal has something in common with the proposals of Storer and Duncan [8, 10]. Like their system, it allows voting by telephone. We consider this to be an important factor because mobile phones are available to a larger portion of the population than computers, especially in poorer countries. We thus rule out of consideration any procedure that requires voters to have access to personal programmable computing devices. It has to be possible to use simple telephony.

The differences between the systems are that whereas Storer and Duncan's system also involves the use of personal voting cards with unique numbers on them, their system has three numbers: the voter ID number, the Personal Candidate ID Number used to vote for a candidate, and a Receipt ID, which is sent back to confirm the vote. Verification by voters is easier in our system since the voter merely has to look for his or her voter number on the YES and NO lists published after the count. In Storer and Duncan's system the voter verifies by matching the candidate name and RCID tuple on the list, which is harder and more demanding. Most importantly, our system allows and facilitates complete anonymity.

In Storer and Duncan's system, the State posts cards to voters and thus can match the voter to the voter number. They propose a complicated system of subdivision of agencies issuing the numbers to protect anonymity, but the voter still has to take it on trust that these State Agencies are not colluding. In our system the voters can be sure that nobody else knows what their voter number is. This is ensured by the readily understandable process of drawing a card from a pile rather than an incomprehensible and opaque electronic or bureaucratic procedure. Their system is not secure against the insertion of fraudulent votes in the event of collusion between the various State Agencies administering it. Because we have completely anonymous voter numbers, we can allow a fully public audit of the voting results that would detect such fraud.

6 Conclusion

Our aim has been to suggest a technology and set of procedures by which a major democratic deficit of modern society [13, 14] can be addressed. E-voting is in the news regularly, and many articles claim that anonymity and auditability cannot co-exist [15].

In this paper we suggest a mechanism which, whilst it makes limited use of cryptographic techniques in the background, is based around objects and procedures with which voters are currently familiar and which does provide an environment for happy co-existence of anonymity and auditability.

We believe that systems like this hold considerable potential for the extension of democratic participation and control.

References

- [1] M I Finley. Democracy Ancient and Modern. Rutgers University Press, 1985.

- [2] Aristotle. The Athenian Constitution. Penguin, 1984.
- [3] David Evans and Nathanael Paul. Election security: Perception and reality. *IEEE Security & Privacy*, 2(1):24–31, 2004.
- [4] Caltech/MIT Voting Technology Project. Voting -what is, what could be. Technical report, Cal-tech/MIT Voting Technology Project, JULY 2001.
- [5] Klonowski, Kutylowski, Lauks, and Zagorski. A practical voting scheme with receipts. In *ICISC: International Conference on Information Security and Cryptology*. LNCS, 2005.
- [6] J T Bradley, A T Gilmore, and N Thomas. What proof do we prefer? Variants of verifiability in voting. In *Workshop on e-Voting and e-Government in the UK*, pages 58–65, Edinburgh, feb 2006.
- [7] S Ibrahim, M Kamat, M Salleh, and S R A Aziz. Secure e-voting with blind signature. In *4th National Conference on Telecommunication Technology Proceedings*, Shah Alam, Malaysia, 14-15 Jan 2003.
- [8] T Storer and S Duncan. Electronic voting in the uk: Current trends in deployment, requirements and technologies. In A Ghorbani and S Marsh, editors, *Proceedings of the Third Annual Conference on Privacy, Security and Trust*, pages 249–252, St Andrews, New Brunswick, Canada, oct 2005.
- [9] W Pieters. What proof do we prefer? variants of verifiability in voting. In *Workshop on e-Voting and e-Government in the UK*, pages 33–41, Edinburgh, feb 2006.
- [10] T Storer, L Little, and S Duncan. An exploratory study of voter attitudes towards a pollsterless remote voting system. In D Chaum, R Rivest, and P Ryan, editors, *IaVoSS Workshop on Trustworthy Elections (WOTE 06) Pre-Proceedings*, pages 77–86, Robinson College, University of Cambridge, England, jun 2006.
- [11] R K Gibson. Internet Elections: The Voters Viagra? In *Workshop on e-Voting and e-Government in the UK*, pages 70–85, Edinburgh, feb 2006.
- [12] Jonathan Bannet, David W. Price, Algis Rudys, Justin Singer, and Dan S. Wallach. Hack-a-vote: Security issues with electronic voting systems. *IEEE Security & Privacy*, 2(1):32–37, 2004.
- [13] S. Wolin. Fugitive democracy. *Constellations*, 1(1), 1994.
- [14] B S Frey. Direct democracy for a living constitution. Walter Eucken Institut, Freiburg Discussion papers on Constitutional Economics , 04/5.
- [15] Press Association News. Fears e-counting system, 19 April 2007. http://www.channel4.com/news/articles/science_technology/fears+over+ecounting+system/446082